

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO**

IN THE MATTER OF THE SEARCH OF:

**One Samsung A13 cellular telephone with
serial number R5CT63EBXSF recovered from
Earnest Sylver and currently in the custody of
HSI Columbus located at 675 Brooksedge
Boulevard in Westerville, Ohio.**

Case No. 2:22-mj-740

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nate Simon being duly sworn, do hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations (HSI), currently assigned to HSI Columbus, Ohio. I have been employed with HSI since its inception in March 2003. Prior to that I was a criminal investigator and border patrol agent with the Immigration and Naturalization Service beginning in April 2000. As part of my daily duties as an HSI Special Agent (SA), I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252(a) and 2252A(a). I have received training in child pornography and child exploitation investigations and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have written numerous affidavits in support of search and arrest warrants related to investigations of child pornography, online enticement, and other child exploitation crimes. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of search warrants.

PURPOSE OF THE AFFIDAVIT

2. This affidavit is submitted in support of an application for a search warrant for the entire contents of the Samsung A13 cellphone S/N: R5CT63EBXSf (the “**SUBJECT DEVICE**”) recovered from Earnest SYLVER more specifically described in Attachment A of this Affidavit, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a) which items are more specifically described in Attachment B of this Affidavit. The **SUBJECT DEVICE** is currently held in the custody of the HSI Columbus office located at 675 Brooksedge Boulevard, Westerville, Ohio 43081.

3. The statements in this affidavit are based in part on information provided by HSI agents, including those located in Canberra, Australia, the Australian Federal Police (AFP), the Ohio Internet Crimes Against Children (ICAC) Task Force, analysts, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a) (transportation, receipt, distribution, and possession of visual depictions of minors engaged in sexually explicit conduct) are presently located on the **SUBJECT DEVICE**.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

- a. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.
- b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.
- c. 18 U.S.C. § 2252(a)(4) prohibits possessing or accessing with intent to view one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

- 5. The following definitions apply to this Affidavit and Attachment B:
 - a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

- b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.
- c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).
- e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy

disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

- f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- g. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

- h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- i. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- j. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.
- k. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- l. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- m. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

- n. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET,
AND EMAIL**

- 6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:
 - a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four (4) functions in connection with child pornography: production, communication, distribution, and storage.
 - b. Child pornographers can transfer printed photographs into a computer-readable format with a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten (10) years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photographs taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of

data or more, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

- c. A modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, “instant messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte or

larger external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

- e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used; however, evidence of child pornography can be found on the user’s computer or external media in most cases.
- g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this

information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

7. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

8. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **SUBJECT DEVICE**, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

9. I submit that if a storage medium is found in the **SUBJECT DEVICE**, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

- a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer

users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

10. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT DEVICE** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

e. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

11. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

12. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, extracting, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later

review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

13. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

BACKGROUND OF CHAT APPLICATION A¹

14. This investigation involves an online messaging application, herein referred to as Chat Application A. Chat Application A is an online messaging application for smartphones, tablets, and computers. The application is multiplatform with versions available for iOS, Android, Windows, Mac, and Linux. Users can also access Chat Application A from a web browser. Chat Application A stores chats and files on a remote server instead of a user's device, so a user can access everything, except secret chats, from the Internet.

15. Through Chat Application A, users can transmit messages, photos, videos, and other types of files with one another. Chat Application A users can also create and participate in "groups," which allow up to 200,000 users to exchange messages and files. Chat Application A groups can be made private and subject to the supervision of administrators, who can control access to the group and memberships in the group.

16. Chat Application A is free and signing up requires only a supported device and a telephone number. Users typically choose a username to communicate with one another, but usernames are not required. Chat Application A is located outside of the United States, puts a premium on security, and does not cooperate with law enforcement or United States court process.

¹ Law enforcement knows the actual name of Chat Application A; however, the investigation into users of Chat Application A remains ongoing, and public disclosure of Chat Application A's actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual name and other identifying details of Chat Application A remain undisclosed in this affidavit.

PROBABLE CAUSE

17. On February 10, 2022, the Australian Federal Police (AFP) Eastern Command Child Protection Operations (EC CPO) team from Sydney, New South Wales (NSW), arrested and charged a 19-year-old NSW male (the POI) for several online child abuse related offences. During the execution of search warrants at the POI's residence, several electronic devices were examined and found to contain Child Exploitation Material (CEM) as well as several social media chats between the POI and persons yet to be identified, all involving the discussion and/or transmission of CEM.

18. During an examination of the POI's Chat Application A account, a conversation was identified between the POI and username "Earnest", which involved the following details:

- Username: Earnest
- Recorded Telecommunications Service: +1 216 352 9199
- Files Transmitted in Chat: 3 Photos, 490 videos, 7 files, and 142 shared links
- Chats Occurred from 14 March 2021 to 28 March 2022

19. A review of the files transmitted to the POI by "Earnest" revealed them to be predominantly, if not all, CEM. At the time of this report, the last online activity from Earnest was on March 28, 2022, where Earnest sent an unsolicited 115.6GB Mega link suspected to contain CEM.

20. HSI Canberra SA Luke Holloway, utilizing the public records database Accurant, was able to identify the likely subscriber of 216-352-9199 as Ernest Egra SYLVER. The report further showed that SYLVER had been associated with the address 25021 Aurora Road, Trailer

188A, Cleveland, OH since January 2017. In April 2022, SA Holloway contacted SA Jason Guyton to provide this information.

21. On April 14, 2022, SA Guyton served T-Mobile Wireless with a DHS Summons (# ICE-HSI-CL-2022-00585) for cellular phone number: 216-352-9199. T-Mobile Wireless produced subscriber information for the above number which is summarized below:

Name:	Earnest Sylver
Address:	25021 Aurora Road, Trailer 188A, Bedford, OH
Account Establish Date:	09/05/2014 (Active)
Personal Telephone Number:	4402650986
Billing SSN:	XXX-XX-6629 [redacted]
Billing DOB:	XX/XX/1970 [redacted]

22. On April 11, 2022, SA Guyton conducted a check of the Ohio Law Enforcement Gateway (OHLEG) database for Earnest Egra SYLVER. The database revealed a suspended driver's license for Earnest Egra SYLVER (DOB: XX/XX/1970; SSN: XXX-XX-6629 [redacted]), at 25021 Aurora Road, TRLR 188A, Bedford Heights, OH. OHLEG further showed that SYLVER has an active vehicle registration for a 2005 Dodge (Red), at the same address.

23. On April 11, SA Guyton received a National Center for Missing & Exploited Children (NCMEC) Cyber Tipline (CT) Report (#40992564) from Ohio Internet Crimes Against Children (ICAC) Task Force Criminal Analyst (C/A) Caroline Wathey. This CT Report showed that on September 30, 2018, the Electronic Service Provider (ESP) Facebook submitted information

to NCMEC regarding the possible possession, manufacture, and/or distribution of child pornography by the following user:

Name: Earnest Sylver

Mobile Phone: +2163529199

Date of Birth: XX-XX-1970 [redacted]

Email Address: esylver@gmail.com (Verified)

Screen/User Name: earnest.sylver9

IP Address: 107.221.46.152 (Login) 09-29-2018 at 12:50:28 UTC

Estimated Location of 09-30-2018: Warrensville Heights, US

Facebook reported that this account uploaded two (2) files of apparent CEM and shared them with another Facebook user on September 29, 2018, at 15:48:27 and 15:48:28 UTC from IP Address 2607:fb90:a331:9f6d:8c02:2414:62a8:845.

24. SA Guyton reviewed the suspected CEM files that were uploaded by Facebook user “Earnest Sylver” that were contained in CT 40992564. Both files appear to capture the same incident which can be further described as:

- Files 457303927_n.mp4 and 58863309_n.mp4 – these 14 second video files depict a naked early pubescent female (approximately 12 – 13 years old) who is kneeling between the legs of an adult male. The male’s erect penis is visible, and the child is engaging in oral to genital sexual intercourse on the male. The male’s face is not visible, and the camera is focused on the sexual act.

25. As noted above, T-Mobile reported that Earnest SYLVER of Bedford Heights, Ohio, has been the registered subscriber of mobile phone 216-352-9199 since 09/05/2014. This is the same phone number associated with Facebook user “Earnest Sylver.”

26. SA Guyton conducted a check of multiple publicly available websites for IP address 2607:fb90:a331:9f6d:8c02:2414:62a8:845, which as reported by Facebook was used by the “Earnest Sylver” account to upload the files of CEM. All these websites indicate that this IP address belongs to T-Mobile, USA. The corresponding cities listed on the different websites include Chicago, Los Angeles, and Bellevue, WA. Your Affiant knows that mobile phone carriers assign their allotment of IP addresses to multiple users. Therefore, hundreds of different users in various locations throughout the United States could be using the same IP address to access the Internet at the same time. SA Guyton knows that T-Mobile will no longer have records for IP address activity from 2018, so no legal process was served for this IP address.

27. On April 19, 2022, SA Guyton conducted surveillance at 25021 Aurora Road, Trailer 188A, Bedford, OH. At approximately 17:55 hours, SA Guyton observed a red Dodge pick-up truck bearing an Ohio license plate ending in “59” parked directly in front of Trailer 188A. A law enforcement database check showed this vehicle is currently registered (expires 12/19/2023) to Earnest E. Sylver Jr. at 25021 Aurora Rd, Trlr 188A, Bedford Hts, OH 44146.

28. SA Guyton reviewed the conversation and file transmission history for “Earnest” that was provided by EC CPO. The chat history shows that in March 2021, the POI sent a message to “Earnest” reading, “Hi. Wanna trade”, to which “Earnest” replied “Yes”. Over the course of March 2021, the users shared multiple files of suspected CEM to include the following:

- File “DSC_7689” – this 10 minute video file depicts a naked adult male lying on his back with a hood over his head, with a naked toddler female (approximately 3-4 years old) and a naked pubescent female (approximately 14-15 years old). During the video, the adult male rubs the toddler female’s genitals and anus with his hands and penis and attempts to insert his penis inside her. Additionally, the pubescent female engages in oral to genital sexual intercourse with the adult male and masturbates his erect penis.

29. In May 2021, SA Guyton observed a message that “Earnest” sent to the POI reading, “Is this app safe? Encrypted”, to which the POI responded “Yeah”. These users shared files of suspected CEM to include the following:

- File “video_93@18-05-2021_19-17-54” – this 4 minute 58 second video files depicts a prepubescent female who appears to be using a cellphone or other electronic recording device. During the video, the child exposes her genitals to the camera and rubs them her hand. The child also bends over and pulls her buttocks apart exposing her genitals and anus to the camera. At multiple points of the video, the camera is held closely/focused on the child’s genitals and anus.

30. In January 2022, SA Guyton observed that “Earnest” and the POI continued to discuss trading files and your Affiant observed that they shared files of suspected CEM to include the following:

- File “VID_20211215_122211_306” – this 1 minute 16 second video file begins with a toddler aged female child, fully clothed with a pacifier in her mouth, masturbating the erect penis of an adult male. The video then changes to a close-

up of her genitals and the adult male can be observed rubbing his erect penis against her genitals. At the conclusion of the video, the adult male ejaculates on to the carpet.

31. On August 25, 2022, SA Guyton conducted surveillance at 25021 Aurora Road, Trailer 188A, Bedford, OH. At approximately 18:20 hours, your Affiant observed a red Dodge pick-up truck bearing an Ohio license plate ending in "59" parked directly in front of Trailer 188A. A law enforcement database check showed this vehicle is currently registered (expires 12/19/2023) to Earnest E. Sylver Jr. at 25021 Aurora Rd, Trlr 188A, Bedford Hts, OH 44146.

32. On November 1, 2022, SA Guyton conducted surveillance at 25021 Aurora Road, Trailer 188A, Bedford, OH. At approximately 18:15 hours, your Affiant observed a red Dodge pick-up truck bearing an Ohio license plate ending in "59" parked directly in front of Trailer 188A. A law enforcement database check showed this vehicle is currently registered (expires 12/19/2023) to Earnest E. Sylver Jr. at 25021 Aurora Rd, Trlr 188A, Bedford Hts, OH 44146.

33. On November 15, 2022, SA Guyton executed a residential search warrant for evidence related to child exploitation crimes at SYLVER's residence located at 25021 Aurora Road, Trailer 188A, Bedford, OH. A laptop was seized, forensically previewed, and revealed images/videos of child exploitation material. SA Guyton determined SYLVER was not at the residence and called the cellphone number associated with him, 216-352-9199. This is the number also associated with Chat Application A described above. SYLVER answered the phone and indicated he was at the Corrections Training Academy (CTA) located at 11781 St. Rt. 762 Orient, OH 43146. SYLVER was recently hired by the Ohio Department of Rehabilitation and Correction and was undergoing his initial training to become a Corrections Officer.

34. Your Affiant responded to the CTA and conducted a recorded interview of SYLVER. SYLVER was advised of his Miranda Rights and agreed to speak with your Affiant. SYLVER indicated he has lived at 25021 Aurora Rd. Apt. 188A Bedford Heights, OH 44146 for seven years. SYLVER was asked about any cellphone he carries, and he stated that his phone was a Samsung, then changed his story indicating he had an LG. SYLVER confirmed he has used the email address esylver@gmail.com. He denied sending or receiving child exploitation material and requested a lawyer before answering anymore questions.

35. At your Affiants request, SYLVER retrieved his cellphone from a blue Nissan Rogue bearing Ohio license plate HAP 6274. Your Affiant obtained SYLVER's phone, dialed 216-352-9199 which was the phone number attributed to SYLVER during the course of his child exploitation activities on Chat Application A and Facebook, and confirmed SYLVER's phone rang. The **SUBJECT DEVICE**, which was identified as a Samsung A13 cellphone S/N: R5CT63EBXSF, was placed in airplane mode and transported to the HSI Columbus office located at 675 Brooksedge Blvd. Westerville, OH 43081. The **SUBJECT DEVICE** was placed in secure storage pending a request for a search warrant.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS AND/OR
ATTEMPT TO VIEW CHILD PORNOGRAPHY**

36. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess and/or attempt to view child pornography:

- a. Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in

sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Such individuals may possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also

have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

- e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools.

Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.²

- f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, telephone numbers, and usernames of individuals with whom they have been in contact and who share the same interests in child pornography.
- g. Such individuals prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

CONCLUSION

37. Based on the above information, there is probable cause to believe that the Specified Federal Offenses have been violated. Accordingly, this Affiant respectfully requests


² See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

that this Court issue a search warrant for the **SUBJECT DEVICE**, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, which constitute evidence, contraband, fruits, and other items related to violations of the Specified Federal Offenses.



Nate Simon
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 16th day of November, 2022.


Elizabeth A. Preston Deavers
United States Magistrate Judge
